What is claimed is:

1. A security engine management apparatus in network nodes comprising:

a security engine including:

a security instruction and library subsystem for processing every application program and utility that are allowed to access to a system source;

a policy decision subsystem for determining a filtering policy, an intrusion detection policy and an access control policy that are required for detecting and blocking an intrusion into a network;

an authentication and access control subsystem for preventing an unauthorized user from using a system and allowing an authorized user to access to the system in response to an application of the access control policy;

a policy application subsystem for analyzing and applying the policies;

a packet filtering subsystem for receiving an allowed packet and denying a disallowed packet in response to the application of the filtering policy; and

an intrusion analysis and audit trail subsystem for analyzing and coping with the intrusion into the network in response to the application of the intrusion detection policy, and

a security management subsystem for managing the

security engine.

2. The security engine management apparatus in network nodes of claim 1, wherein the policy application subsystem provides intrusion detection and audit information through a device driver and packet statistical information through a proc file system to the policy decision system.

3. The security engine management apparatus in network nodes of claim 1, wherein the filtering policy is used for blocking or passing a packet having a certain destination address depending on a sender address, a destination address, a sender port, a destination port, and a protocol type.

4. The security engine management apparatus in network nodes of claim 1, wherein the intrusion detection policy includes rules for detecting a DoS attack and a specific virus pattern.

5. The security engine management apparatus in network nodes of claim 1, wherein in case the virus file is downloaded, the intrusion analysis and audit trail subsystem detects the virus file transfer by examining a file pattern and then informs the virus file transfer on a mobile terminal; and in case the DoS attack is attempted, the intrusion analysis and audit trail subsystem examines a DoS

attack pattern to block the DoS attack, thereby storing detection information on the DoS attack and the virus attack in an audit recording database.

6. The security engine management apparatus in network nodes of claim 1, wherein the security management subsystem further includes:

a security management GUI of a web base, for executing a management instruction;

an audit management module for processing audit information on an illegal intrusion;

a log-in processing module for performing a user authentication by using a user ID and a password inputted from the mobile terminal;

a packet statistical module for showing packet statistical information on each of protocols and an interfaces;

a network setting module for showing a network status for routers and systems through the security management GUI;

a policy management module for displaying a security policy for detecting a network intrusion and performing an addition, a deletion, and an edition thereof;

an audit management module for displaying information on the DoS attack and the virus attack on the mobile terminal by using a short message service (SMS); and

a network communication module for communicating with

the policy decision subsystem for a policy management and informing the audit management module of the policies in real time.

7. The security engine management apparatus in network nodes of claim 6, wherein the network setting module displays network interface information on an interface card type, an IP address, a hardware address, and a size, state and option of maximum transmission unit (MTU), and system information on OS information, a booting elapsed time, a current time, a system name, and a disc size, and performs an addition, a deletion, and an edition of a routing table.

8. The security engine management apparatus in network nodes of claim 6, wherein in case an intrusion occurs during an off state, the policy management module only detects the intrusion; and in case the intrusion is detected during an on state, the policy management module informs the mobile terminal of the intrusion by using an SMS and then discards the intrusion packet.

9. A method for security engine management in network nodes, comprising the steps of:

(a) receiving a packet from an attack system and examining the packet according to a filtering policy;

(b) checking whether the packet is allowed or not,

based on the examination result of step (a);

(c) passing the packet if the packet is allowed in the step (b) and checking whether or not the allowed packet is an attack intrusion packet according to an intrusion detection policy; and

(d) in case the packet is the attack intrusion packet in the step (c), displaying the attack intrusion packet on a security management GUI and informing a mobile terminal by using an SMS and denying the corresponding packet.

10. The security engine management method in network nodes of claim 9, wherein if the packet is disallowed in the step (b), the disallowed packet is denied.

11. The security engine management method in network nodes of claim 9, wherein if the packet is a general packet in the step (c), the packet is transferred through a network.

12. A method for providing an integrative security management by using a security policy applied between a router and a security management subsystem, the method comprising the steps of:

(a) checking whether or not a user is authorized through a user registration and authentication process;

(b) if the user is authorized in step (a), allowing a user to access to the security management subsystem,

collecting information on a network composition of hosts, gateways, and routers and storing the collected information in a network database; and

(c) displaying security management information on a security management GUI.

13. The method of claim 12, wherein if the user is not authorized in the step (a), the user is blocked to access to the security management subsystem and system sources of network nodes to prevent damage generated by an illegal acquisition of a root authority.

14. The method of claim 13, wherein if the user is not authorized in the step (a), a security engine is managed based on a security policy and the security policy is stored in a policy database.

15. A recording medium for recording therein a program for implementing a method of claim 9.

16. A recording medium for recording therein a program for implementing a method of claim 12.